a^1 con't

one or more buses for connecting the internal memory unit, the processor, the tamper detection and response logic, and the interface to external systems and components;

a memory management unit;

a level-one page table, the level-one page table including a plurality of level-one page table entries, wherein the level-one page table entries each correspond to at least one level-two page table, and wherein the level-one page table entries each contain a predefined attribute, the predefined attribute being operable to indicate to the memory management unit whether entries in a corresponding level-two page table may designate certain predefined memory regions;

a plurality of processor security registers; and

a tamper-resistant housing.

a^2

7. A secure processing unit as in claim 1, further comprising:

access control data, the access control data being operable to indicate whether access to predefined memory regions is restricted to certain software components or processor modes.

a^3

10. A secure processing unit as in claim 1, whereby level-two page tables that may not designate the predefined memory regions are not stored in the internal memory unit.

11. An information appliance comprising:

a memory unit;

a secure processing unit comprising:

a3 cont

a tamper resistant packaging,

tamper detection and response logic,

a secure memory unit, and

a processing unit, including a memory management unit and a plurality of processor security registers;

a level-one page table and a plurality of level-two page tables, the level-one page table including a plurality of level-one page table entries and the level-two page table including a plurality of level-two page table entries, wherein the level-one page table entries each correspond to at least one level-two page table, and wherein the level-one page table entries each contain a predefined attribute, the predefined attribute being operable to indicate to the memory management unit whether a corresponding level-two page table may designate certain predefined memory regions; and

a bus for connecting the memory unit and the secure processing unit;

wherein the secure processing unit is operable to perform both secure processing operations and at least some processing operations performed by a conventional information appliance processing unit.

a4

18. An information appliance as in claim 11, in which level-two page tables that may not designate the predefined memory regions are stored in the memory unit, and wherein the level-one page table and the level-two page tables that may designate the predefined memory regions are stored in the secure memory unit.